https://doi.org/10.7840/kics.2024.49.5.726

인지 무선 네트워크의 군사적 적용 가능성에 대한 조사

리차드 로시◆, 클레망 디바르부이*, 김 용 철°

A Survey on Potential Military Application of Cognitive Radio Networks

Richard Losi◆, Clément Débarbouillé*, Yongchul Kim°

요 약

인지 무선 네트워크(CRN)는 스펙트럼을 효과적으로 활용하는 적응형 네트워크 기술이다. 이 기술은 아직 완전하진 않지만 일부 민간 영역에서 먼저 사용되기 시작하였고, 그러므로 군에서 직면해야 하는 주요 위협인 전파 방해 또는 스푸핑에 대비하여 이 기술을 사용하는 것은 매우 흥미로운 주제이다. 본 연구에서 우리는 CRN의 특징과 관련하여 모든 유형을 조사하여 분석하였다. 실제로 CRN의 종류는 매우 다양하고, 각 CRN에는 장점과 약점을 제공하는 고유한 특성과 고유한 아키텍처가 있다. 군에 적용 가능한 CRN을 제안하기 위하여 다양한 공격에 대해 여러 유형의 통신 링크 시나리오를 제시하고 각각의 통신 링크의 특성에 적합한 CRN 카테고리를 제시하고자 하였다.

Key Words : Cognitive Radio, Channel-Hopping, Rendezvous Algorithm, Spoofing

ABSTRACT

Cognitive radio networks (CRNs) are an adaptative type of network that better the use of the spectrum. This technology is not completely ready yet, but its implementation has begun in some civilian areas. That is why their use in the military could be interesting, against jamming or spoofing for instance that are the major threats Armed Forces must face. We have studied and classified all the types of CRNs regarding their features. In fact, there are many different types of CRNs, and each CRN has its own characteristics and unique architecture that provides strengths and weaknesses. To propose CRNs applicable to the military, we attempted to present several types of communication link scenarios for various attacks and present CRN categories appropriate for the characteristics of each communication link.

Ⅰ. Introduction

The field of communications has undergone many changes over the centuries. The arrival of wireless communications revolutionized civil communications. In the military field, this evolution has revolutionized the fight. As combatants became able to communicate with each other through wireless communication even if they were not within visible or audible distance, the movement of units during combat became faster

※ 본 논문은 육군사관학교 화랑대연구소의 2024년도 연구활동비 지원을 받아 연구되었음.

◆ First Author : Korea Military Academy Department of Electrical Engineering, richardlosi38@gmail.com, 정회원

° Corresponding Author : (ORCID:0000-0003-1393-8711)Korea Military Academy Department of Electrical Engineering, kyc6454@gmail.com, 종신회원

* Korea Military Academy Department of Electrical Engineering, clm.debarbouille@gmail.com

논문번호 : 202310-117-C-RN, Received October 29, 2023; Revised January 3, 2024; Accepted January 24, 2024

and the scope of the battlefield greatly expanded. Indeed, the ability to communicate is key on the battlefield. Many examples can show their importance, from the Marathon messenger to the great headquarters of transmission in the sub-Saharan band through the carrier pigeons of the fort of Vaux during the Great War, transmissions play a decisive role in future battles.

In this ever-evolving landscape of wireless communication, CRNs (Cognitive Radio Networks) emerge as a cutting-edge technology, promising to optimize the use of the radio spectrum. Already extensively explored for their potential in the civil sector, they have showcased their value in scenarios where agility, flexibility, and spectrum optimization are paramount. Even in 5G networks that offer higher data rates, ubiquitous connectivity, lower end-to-end latency, much higher system capacity, and improved energy efficiency, CR technology can provide dynamic spectrum sharing to achieve higher spectral efficiency[8,9].

If some civil applications have already demonstrated the potential of CRN, it's only logical to envision their adoption in a military context. Armed Forces, always in search of more robust, secure, and adaptive ways of communication, could greatly benefit from this technology. The U.S.'s Joint Tactical Radio System (JTRS) program, has explored this avenue, underscoring the military's aspiration to integrate CRN to meet its unique and demanding requirements.

Ⅱ. Taxonomy of CRNs.

2.1 How CRNs work.

CRNs represent a technological advance designed to improve the use of the radio spectrum. Rather than being restricted to a fixed frequency band, a CRN can intelligently detect and operate unused portions of the radio spectrum. It dynamically adapts to its environment by constantly evaluating the conditions of the spectrum and adjusting its transmission accordingly. The motivation behind this technology is the finding that many frequency bands are underutilized by primary users (PUs). CRNs therefore seek to maximize the use of the available spectrum without causing trouble with primary users.

To create a communication, the secondary users (SUs) will analyze the spectrum to find free channels and move from one channel to another in order to create a link with other SUs, it is the phenomenon of hopping. The different SUs do not know if other SUs want to communicate with them, their search is then completely independent of the other SUs. When two SUs manage to find a free channel to communicate, this is called a rendezvous as shown in Figure 1. Before each communication, there is a waiting time before both SUs can rendezvous, this is called the Time-to-Rendezvous (TTR).

CRNs can be classified based on various criteria, particularly on how they manage coordination and communication between users. The architecture between two CRNs algorithms can be very different. Figure 2 is a taxonomy of different CRNs categories from [1] :

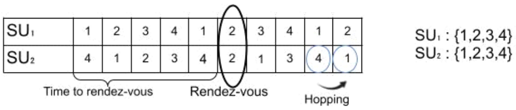


Fig. 1. How a CRN works.

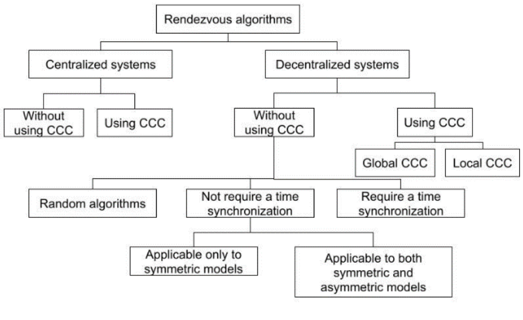

Rendezvous algorithms
Centralized systems
Decentralized systems
Without using CCC
Using CCC
Without using CCC
Using CCC
Global CCC
Local CCC
Random algorithms
Not require a time synchronization
Require a time synchronization
Applicable only to symmetric models
Applicable to both symmetric and asymmetric models

Fig. 2. Taxonomy of rendezvous algorithms.

2.2 Centralized CRNs.

Centralized CRNs, as shown in Figure 3, are part of a network where all decisions regarding channel selection, resource management, PUs detection and other functions are made by a central entity, this is the access point. As centralized CRNs, we can

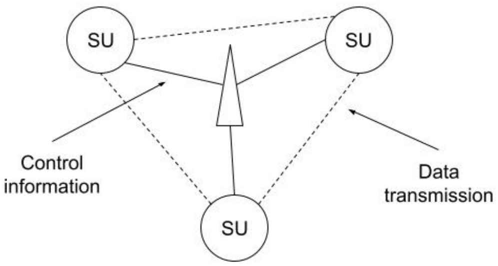


Fig. 3. A centralized CRN.

distinguish between CRNs that use a CCC (Common Control Channel) and those that do not. The CCC is a specifically designated channel that all network users, whether primary or secondary, use to exchange control information.

The great advantage of using a CCC is to facilitate coordination between users so as to drastically reduce the TTR. However, it is also a network weakness because this channel is a single point of failure that can be jammed, and the network cannot work. However, this architecture of the network is particularly strong against spoofing because this permanent link between users and the central entity allows to easily detect intrusion from a malicious user. Nowadays this type of CRN is used for civilian applications, one of the best examples of centralized network usage with CCC is 5G[2].

2.3 Decentralized CRNs.

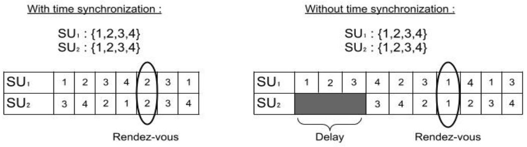
A decentralized CRN is a configuration where there is no central entity to oversee and control the network. Instead, each user operates autonomously, making its own decisions about spectrum detection and channel selection. The distinction between networks with CCC and without CCC can also be made

Regarding a military use, decentralized CRNs with CCC do not appear useful because there are still the issues of a central point of failure without the strengths of a centralized network. So, it would not give any concrete advantage to the network, which is why we will focus on decentralized CRNs without CCC. There are 3 types of these networks: networks with synchronization, those without, and random networks. Random CRNs are randomly choosing the channel beyond the available channels. The main issue with this type of algorithm is that the TTR can be very long, and you are not sure to finally reach a rendezvous.

The difference between CRNs with and without synchronization is explained in Figure 4. Indeed, CRNs with sync have a common knowledge of time and adopt common schemes to hop between channels. This increases the likelihood of finding a rendezvous. CRNs without synchronization have methods that maximize the probability of rendezvous, but users do not have the same time origin, this is less effective in finding a rendezvous, but it does not require synchronization. This type of network has been used following the earthquake in Haiti in 2010 by the rescue teams to overcome damaged infrastructure.

However, one of the major difficulties is that two SUs will not have the same channels available, in the asymmetric case. In the example shown in Figure 5, SU1 has access to the bands {1,2,3,4} and SU2 has access to the bands {5,2,6,8,}. For an insured rendezvous, it is necessary that both users have at least one common channel, but the others can be different, and the total number of channels can be different for both users.

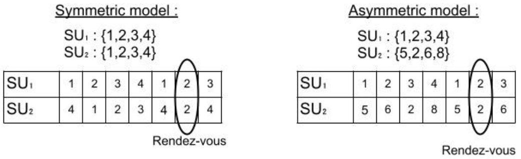
The diversity of algorithms shows the adaptability of this new type of communication which is already used in civil applications. Whether centralized or decentralized, with CCC or without CCC, CRNs provide optimized communications to cope with any type of environment. We can naturally wonder whether this type of communication would be



SU_1	1	2	3	4	2	3	1
SU_2	3	4	2	1	2	3	4

SU_1	1	2	3	4	2	3	1	4	1	3
SU_2	▨	▨	▨	3	4	2	1	2	3	4

Fig. 4. Synchronized and asynchronized CRNs.



SU_1	1	2	3	4	1	2	3
SU_2	4	1	2	3	4	2	4

SU_1	1	2	3	4	1	2	3
SU_2	5	6	2	8	5	2	6

Fig. 5. Symmetric and asymmetric models.

effective for military applications where the constraints and the needs are different.

Ⅲ. Issues with CRNs.

3.1 Security.

According to [3], security is a key point for CRNs. In fact, CRNs are vulnerable to a large scope of classic attacks such as Sybil attacks or wormhole attacks. More precisely, in a CRN, users are dynamically using the spectrum, and all users are connected together to exchange information. So, if one of the users is corrupt, it hurts the whole network. Moreover, people can create a malicious user and deter the network with it. In CRNs, a malicious person manages to modify the spectrum for some users, it could greatly deter communication and sometimes avoid it. In addition, if a malicious user manages to pretend to be a primary user, it can avoid access to some channels too.

3.2 Ability to detect free channels and hop to them.

CRNs have been created to find a free channel and to better the use of the spectrum by detecting if a primary user is using a frequency. However, the world is more and more connected, and the spectrum begins to be overcrowded. So, there are free channels only if primary users are not using them. It means that, in the future, the availability of the spectrum is not ensured. Even if there are moments for secondary users to hop on a channel and communicate on it, the global number of primary users can deter the communication between secondary users and highly increase the TTR. It takes time for a user to detect a free channel and hop to it, the time taken for that could be longer than the time when the channel is free.

The overlay access to the spectrum mentioned in [7] puts on the table the ability to detect if a primary user is using the channel or not and if users are able to send the right amount of energy to communicate with another user without disturbing it. In fact, what is limiting the implementation of CRNs is also the technological progress in spectrum detection.

3.3 Ability to rendezvous quickly.

Reducing the TTR is a key to ensure a good communication between users. As cognitive radios strive to agree on a specific communication channel in a tight timeframe, several interconnected obstacles emerge [4]. In fact, the algorithms implemented for CRNs are really complex and this complexity increases the time needed to find a rendezvous. The algorithms must consider several factors to work. The operation of searching a free channel across the available channels takes time. Moreover, changes in the spectrum landscape force the secondary users to adapt themselves to the current situation. In a way, the implementation of CRNs relies on the power of computers used.

All of the operations to rendezvous take time : searching a free channel, seeing if another secondary user is there, hopping on this channel, and then communicating with it. This latency is accumulating and deters the quality of the network by increasing the TTR.

3.4 Adaptability to existing networks.

The transition to CRNs presents notable challenges, particularly when considering system architectures. Many modern systems are rigid in design, and embedding cognitive radios may need deep modifications. CRNs employ advanced techniques tailored for efficient spectrum use, but these can conflict with established systems. For instance, melding CRNs into a 4G cellular network might compel extensive modifications [5], both in base stations and user devices. Additionally, software would need updates to support CRN functionalities.

In summary, CRNs are a technology that requires more and more complex systems to be implemented. This is mainly due to the complex management of the spectrum and the ability to find a rendezvous quickly between two users. Moreover, there are a lot of security issues with CRNs that must be fixed, especially for military applications. However, CRNs are really interesting in their management of the spectrum, particularly in a disturbed environment. That is why we will focus on which type of CRN can be implemented in the armed forces and in which field.

Ⅳ. Which type of CRN for the military.

The military world has many constraints in terms of communication but the use of CRNs could bring better adaptability and therefore better performance to networks. Different studies have investigated their potential for use in the military world [6], we propose in this part a potential use in a high-intensity scenario where we can find different types of environments that will vary the expectations and characteristics of communications. After describing this fictitious scenario we have assigned for each link a type of CRN algorithm that is most suitable for the link.

4.1 Description of a high-intensity war scenario.

Imagine a country separated in two for more than 70 years, the South then decides to unify the country by recovering the territories of the North. For this, the South carried out a large-scale joint military operation. The main objective of the troops of the South was to quickly seize the capital of the North. To do this, the main HQ (Headquarter) located in the capital of the South decided to create an operational HQ just north of the border in a space secured by previous fighting. This operational HQ commands all the fighting forces composed of a cavalry regiment and an infantry regiment whose mission is to seize the capital of the country. These troops are supported by a fleet of the National Navy and a fighter group of the Air Force. In addition, a special forces regiment is tasked with covering the North, from which could arrive enemy reinforcements. We imagine in our scenario that all communications are done through CRNs either in the different units or between them. The scenario and the communications between the units are represented in Figure 6.

There are two main types of attacks against CRNs: jamming and spoofing. We believe that a jamming attack can be fast but requires to be quite close to your target to reach an effective jamming. A spoofing attack is less fast but is a long-range attack type. It means that the enemy would take control of a user and will then use it to deter the network or create a new user and try to enter in our network to disturb it. Regarding those threats, we have chosen which threat in prominent for each link and we have picked the right type of CRN for each communication.

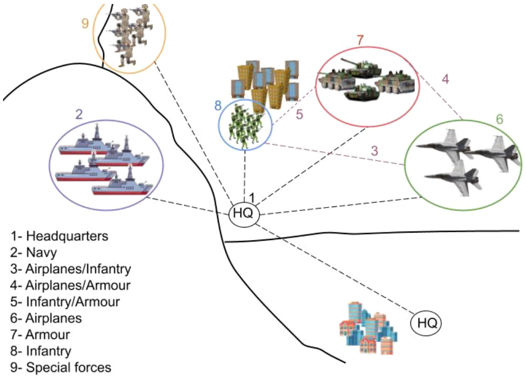


Fig. 6. A high-intensity war scenario.

4.2 Links between HQ and the others.

The HQs we consider are far from the front line. That is why we believe that the main threat is a spoofing attack because they are not close enough to the enemy to be jammed. Then, the network should be able to detect an intrusion from a spoofed user or from a user that has been hacked or physically taken by the enemy so as to ensure its own security. In fact, the link between those kinds of HQs should be really secured because it contains strategic information. That is why the main quality of this network should be its security, especially against spoofing which is its major threat.

In order to ensure this level of security, it is better to use a centralized network with a CCC. Firstly, because the centralization connects all the users with a gateway, so it is easier to detect if something is going wrong with a user or to detect if an enemy is trying to enter in our network. Whereas in a decentralized network, each user is not aware of the existence of other users. Therefore, it is easier for the enemy to create a corrupt user and enter in our network. For those reasons, the American armed forces had chosen to develop only centralized CRNs with CCC in their JTRS program.

In addition, a centralized CRN allows the TTR to be very low. So, this kind of network would be suitable for real-time communication and also for big data exchanges (sending a document or a video for instance).

4.3 Links inside the Navy.

We believe that the Navy would be more subject to spoofing than jamming because of its location on the battlefield. Jammers are types of equipment located next to the frontline and a jammer embarked on a ship is not likely to be efficient. More precisely, if a ship wants to use its jammer against our ship, it should be quite close to it, but it would have been detected by our own ship. It means that it is harder to be stealthy over the sea. However, it is not so hard to be stealthy under the sea. So, a jammer embarked on a submarine could be effective. But the submarine would be detected as soon as the jammer is used so this option is not likely to happen. Finally, the major threat for boats is spoofing and especially the creation of a corrupt user.

That is why a centralized CRN with CCC is the best option. It allows a proficient level of security against spoofing and a good channel hopping speed so as to communicate quickly with other users with a great quantity of data. Moreover, one ship can play the role of the gateway for this CRN and this gateway can be a user of the CRN linked with the HQ. The use of a CRN could bring some benefits to the Navy particularly if the network is busy, next to the coast or near allied ships for instance.

4.4 The links Air Force-Armour-Infantry.

The range of fire of the K9 Thunder is 40 km. It is 70 km for the French CESAR. Therefore, according to us, any gateway within 100 km from the front is vulnerable. That is why we think that the Army and the Air Force cannot rely on gateways to communicate. Users should be independent to ensure the survivability of the network. Decentralized CRNs are thus appropriate for this use. In addition, the main threat is jamming because units are just next to the front line. Using a CCC would be an issue because if the enemy finds the working frequency of the CCC, the whole network is lost.

Moreover, those links between infantry and the armour for instance must be relatively quick. In fact, the space-time frame is reduced at the tactical scale. To ensure a good TTR, it is better to choose a decentralized CRN with time synchronization. This synchronization could occur during the preparation phases of the conflict for example. If it is not possible, a decentralized CRN without time synchronization would still be efficient.

The main drawback of this type of CRN is that the TTR can be long. So, the best use of this technology in this case would be to send large-volume documents that do not need to be sent very quickly. Real-time communication may not be the best idea in this case.

4.5 Links inside the infantry and the armour.

Combat branches are obviously just next to the front line. This proximity involves that the main threat will be jamming in communications. Moreover, the space-time frame is really reduced, and decisions and orders must be given very quickly. That is why relying on a CRN to communicate in this case can appear to not be really interesting, because the information given by radio is important for the maneuverer but does not have a strategic interest.

In fact, a CRN could be useful for sending videos of the fight for instance. Therefore, the information sent by this network must be sent more quickly than in a combined or joint network because of the reactivity of the battlefield. That is why we pick a decentralized CRN without CCC with time synchronization in this case. The decentralized network offers great resistance to jamming because of its use of the spectrum. Using a CCC would be a mistake because the enemy jammer could find the working frequency of the CCC and jam it. A synchronized network would allow a lower TTR.

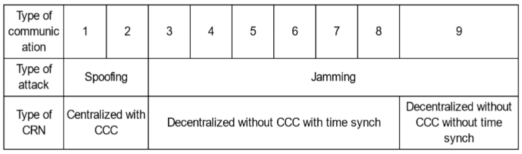
This type of network is particularly interesting for combat branches because of its resilience. The war in Ukraine shows the importance of electronic warfare. Even if the communication could be slower due to the TTR, this type of network allows units to continue to communicate despite jamming.

4.6 Links within the Special Forces units.

This unit's mission is to monitor an area from which enemy reinforcements could come. It consists of informing any movement coming from the North. The major threat is jamming because the unit is behind the frontline. There are also other networks working such as 5G and TV broadcasting. Consequently, the spectrum can be overcrowded but these units still need to communicate. The speed of the communication is not particularly important because there is no idea of movement for groups monitoring a zone. However, it is key to communicate and if possible, to not be detected.

A decentralized CRN without CCC and without time synchronization offers a good resistance to jamming, a good use of the spectrum, and a great adaptability. Special forces units will be able to communicate despite jamming and an overcrowded spectrum.

In general, tactical situations are quite different on the battlefield specifically in a high-intensity war. The use of CRNs could allow forces to adapt to the situation and the different threats of the environment. This technology could be better adapted to different terrains (desert, urban, equatorial) than current systems thanks to its dynamic selection of the channel which could increase the resistance of the network to jamming or spoofing. Figure 7 shows a summary of the algorithms suitable for each link mentioned so far and the types of vulnerable attacks.



Type of communication	1	2	3	4	5	6	7	8	9
Type of attack	Spoofing		Jamming						
Type of CRN	Centralized with CCC		Decentralized without CCC with time synch						Decentralized without CCC without time synch

Fig. 7. Type of algorithm chosen regarding the link and the most likely attack.

Ⅴ. Conclusion

In conclusion, this study presents a taxonomy of existing CRNs and what is currently limiting their use. The purpose of this study is to determine whether CRN can be used in the military field. To this end, we imagined complex high-intensity networks and studied various communication cases to see whether the use of CRNs would or would not be helpful, and if so, which types of CRNs would be most effective. The variety of scenarios allowed us to demonstrate all the advantages over the use of traditional military radios. Although we are aware that the application of CRNs will be difficult in the military field, this study shows that the application of CRN is feasible and can bring benefits.

References

[1] H. Liu and Z. Lin, X. Chu, and Y.-W. Leung "Taxonomy and challenges of rendezvous algorithms in cognitive radio networks," *Int. Conf. Comput., Net. and Commun. Invited Position Paper Track*, Jan. 2012. (https://doi.org/10.1109/ICCNC.2012.6167502)

[2] V. S. Ramaiah, B. Singh, A. R. Raju, G. N. Reddy, K. Saikumar, and D. Ratnayake, "Teaching and learning based 5G cognitive radio application for future application," *ICCIKE*, Mar. 2021. (https://doi.org/10.1109/ICCIKE51210.2021.9410797)

[3] H. Idoudi, K. Daimi, and M. Saed, "Security challenges in cognitive radio networks," *The 2014 ICISIE*, Jul. 2014.

[4] M. Suriya and M. G. Sumithra, "Overview of spectrum sharing and dynamic spectrum allocation schemes in cognitive radio networks," *8th ICACCS*, Mar. 2022. (https://doi.org/10.1109/ICACCS54159.2022.9785048)

[5] Y. Shivam, K. Prashant, K. S. Ravi, R. Vivek, and P. Devasis, "A detail survey of channel access method for cognitive radio network (CRN) applications toward 4G," *South Asian Res. J. Eng. and Technol.*, vol. 3, no. 1, Jan. 2021. (https://doi.org/10.36346/sarjet.2021.v03i01.005)

[6] V. Speybrouck, E. Despoux, and Y. Kim, "A study on the use of cognitive radio networks

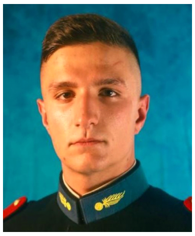
in the military operation environment," *J. Convergence for Inform. Technol.*, vol. 11, no. 12, Dec. 2021. (https://doi.org/10.22156/CS4SMB.2021.11.12.106)

[7] B. Bharti, P. Thakur, and G. Singh, "A framework for spectrum sharing in cognitive radio networks for military applications," *IEEE Potentials*, vol. 40, no. 5, pp. 39-47, Sep. 2021. (https://doi.org/10.1109/MPOT.2017.2751656)

[8] S. Sasipriya and R. Vigneshram, "An overview of cognitive radio in 5G wireless communications," *IEEE Int. Conf. Comput. Intell. and Comput. Research (ICCIC)*, Chennai, India, Dec. 2016. (https://doi.org/10.1109/ICCIC.2016.7919725)

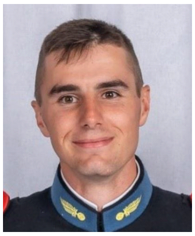
[9] S. Bhandari and S. Joshi, "Cognitive radio technology in 5G wireless communications," *IEEE ICPEICES*, Delhi, India, Oct. 2018. (https://doi.org/10.1109/ICPEICES.2018.8897345)

리차드 로시 (Richard Losi)



He was born in Grenoble, Rhone-Alpes, France, in 2001. Second Lieutenant at the French Military Academy, he is specialized in electrical engineering. He is currently pursuing the master degree.

클레망 데바르부이 (Clément Débarbouillé)



He was born in Beaune, Burgundy, France, in 2001. Second Lieutenant at the French Military Academy, he is specialized in electrical engineering. He is currently pursuing the master degree.

김 용 철 (Yongchul Kim)

1998년 3월 : 육군사관학교 전자공학과 학사

2001년 11월 : University of Surrey, UK 전자공학과 석사

2011년 12월 : North Carolina State University, USA 전기컴퓨터 공학과 박사

2012년 2월~현재 : 육군사관학교 전자공학과 부교수

<관심분야> WiMAX, Relay Networks, Ad-hoc Networks, Wireless Jamming.